Assurance report

any.cloud A/S

Independent auditor's ISAE 3000 assurance report with reasonable assurance, on information security and measures pursuant to the data processing agreements with customers throughout the period from 20 April 2023 to 19 April 2024

April 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of Contents

Section 1: any.cloud A/S' statement

The accompanying description has been prepared for data controllers, who has signed a data processing agreement with any.cloud A/S, and who has a sufficient understanding to consider the description along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the EU Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter "the Regulation") have been complied with.

Some of the control areas, stated in any.cloud A/S' description in Section 3 of SaaS data security services, can only be achieved if the complementary controls with the customers are suitably designed and operationally effective with any.cloud A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary controls.

any.cloud A/S confirms that:

a) The accompanying description, Section 3, fairly presents how any.cloud A/S has processed personal data for data controllers subject to the Regulation throughout the period from 20 April 2023 to 19 April 2024. The criteria used in making this statement were that the accompanying description:

(i) Presents how any.cloud A/S' processes and controls were designed and implemented, including:

- The types of services provided, including the type of personal data processed
- The procedures, within both information technology and manual systems, used to initiate, record, process and, if necessary, correct, delete, and restrict processing of personal data
- The procedures used to ensure that data processing has taken place in accordance with contract, instructions, or agreement with the data controller
- The procedures ensuring that the persons authorised to process personal data have committed to confidentiality or are subject to an appropriate statutory duty of confidentiality
- The procedures ensuring upon discontinuation of data processing that, by choice of the data controller, all personal data are deleted or returned to the data controller unless retention of such personal data is required by law or regulation
- The procedures supporting, in the event of breach of personal data security, that the data controller may report this to the supervisory authority and inform the data subjects
- The procedures ensuring appropriate technical and organisational safeguards in the processing of personal data in consideration of the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed
- Controls that we, in reference to the scope of SaaS data security services, have assumed would be implemented by the data controllers and which, if necessary, in order to achieve the control objectives stated in the description, are identified in the description
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that are relevant to the processing of personal data

(ii) Includes relevant information about changes in the data processor's SaaS data security services in the processing of personal data throughout the period from 20 April 2023 to 19 April 2024;

(iii) Does not omit or distort information relevant to the scope of SaaS data security services being described for the processing of personal data while acknowledging that the description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of SaaS data security services that the individual data controllers might consider important in their particular circumstances.

b) The controls related to the control objectives stated in the accompanying description were, in our view, suitably designed and operated effectively throughout the period from 20 April 2023 to 19 April 2024; if the data controller has performed the complementary controls, assumed in the design of any.cloud A/S' controls as of 20 April 2023 to 19 April 2024. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 20 April 2023 to 19 April 2024.

c) Appropriate technical and organisational safeguards were established and maintained to comply with the agreements with the data controllers, sound data processing practices and relevant requirements for data processors in accordance with the Regulation.

Copenhagen, 29 April 2024
any.cloud A/S

Gregor Frimodt-Møller
Group CEO

Section 2: Independent auditor's ISAE 3000 assurance report with reasonable assurance on information security and measures pursuant to any.cloud A/S' data processing agreements with customers throughout the period from 20 April 2023 to 19 April 2024

To: any.cloud A/S and their customers

Scope

We were engaged to provide assurance about a) any.cloud A/S' description, Section 3 of SaaS data security services in accordance with the data processing agreement with customers throughout the period from 20 April 2023 to 19 April 2024 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the Description.

Some of the control objectives stated in any.cloud A/S' description in Section 3 of SaaS data security services, can only be achieved if the complementary controls with the customers have been appropriately designed and operating effectively with the controls with any.cloud A/S. The report does not include the appropriateness of the design and operational effectiveness of these complementary controls.

We express reasonable assurance in our conclusion.

any.cloud A/S' responsibilities

any.cloud A/S is responsible for: preparing the description in Section 3, and the accompanying statement in Section 1, including the completeness, accuracy, and the method of presentation of the description and statement, providing the services covered by the description; stating the control objectives; and for the design and implementation of operationally effective controls, to achieve the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark.

Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on any.cloud A/S' description and on the design and operational effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3000, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information", and additional requirements under Danish audit regulation, to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are appropriately designed and operating effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a data processor involves performing procedures to obtain evidence about the disclosures in the data processor's description of its SaaS data security services and about the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not appropriately designed or operating effectively. Our procedures

included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the appropriateness of the objectives stated therein, and the appropriateness of the criteria specified by the data processor and described in Section 1.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a data processor

any.cloud A/S' description is prepared to meet the common needs of a broad range of data controllers and may not, therefore, include every aspect of SaaS data security services that the individual data controller may consider important in their particular circumstances. Also, because of their nature, controls at a data processor may not prevent or detect personal data breaches. Furthermore, the projection of any evaluation of the operating effectiveness to future periods is subject to the risk that controls at a data processor may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the *Management's statement* Section 1. In our opinion, in all material respects:

(a) The description fairly presents SaaS data security services as designed and implemented throughout the period from 20 April 2023 to 19 April 2024;

(b) The controls related to the control objectives stated in the description were appropriately designed throughout the period from 20 April 2023 to 19 April 2024, and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 20 April 2023 to 19 April 2024.

Description of tests of controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4.

Intended users and purpose

This report and the description of tests of controls in Section 4 are intended only for data controllers who have used any.cloud A/S' SaaS data security services who have a sufficient understanding to consider it along with other information, including information about controls operated by the data controllers themselves in assessing whether the requirements of the Regulation have been complied with.

Copenhagen, 29 April 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: any.cloud A/S' description of processing activity for the supply of SaaS data security services

The purpose of this description is to provide information to any.cloud's customers and their stakeholders (including auditors) about compliance with the content of the data processing agreement ("DPA").

In addition, the purpose of this description is to provide information on processing security, technical and organisational measures, and responsibilities between the data controllers (our customers) and any.cloud.

Description of control environment for any.cloud

Introduction

The purpose of this description is to provide information to any.cloud's customers and their stakeholders (including auditors) about compliance with the content of the data processing agreement ("DPA").

In addition, the purpose of this description is to provide information on processing security, technical and organisational measures, and responsibilities between the data controllers (our customers) and any.cloud.

The description is also intended to provide information about the controls used for services at our premises during the period.

The description includes the control objectives and controls at any.cloud, which cover our customers and are based on our standard delivery.

any.cloud delivers professional ISO-certified SaaS data security services to companies in Denmark and abroad using a channel strategy. any.cloud's Danish infrastructure is hosted in Digital Realty Denmark in Ballerup. In addition, any.cloud uses IBM Cloud data centres to provide services that, with 60+ data centres spread over 30+ countries, make any.cloud an international company that provides services worldwide.

In recent years, any.cloud has not only grown and scaled its business and organisation in preparation for increasing international demand but has also made significant improvements in terms of the quality of its services.

any.cloud has become a market leader within its field and also compliant with the vast majority of customers with its ISO 27001, ISAE 3000 GDPR and CSA certification. any.cloud is required to conduct business in accordance with strict control measures, high security requirements and transparency in terms of the quality and security in its IT services. This ensures that we constantly maintain the quality required to be one of the leading vendors of Cloud services.

any.cloud uses the best suppliers to deliver the highest quality Cloud services and uses uncomplicated and innovative solutions to meet the needs of customers. Through scalable business continuity, financial transparency and the will and ability to take responsibility for the environmental aspects of running our business, we contribute to our customers' business and growth. We set ourselves apart from other players in the market through our simple price structure, superior quality of service, international distribution strategy, focus on personal relationships and our direct access to specialists, which allows us to offer our end customers very short response times.

any.cloud's ability to give the end customer a high-quality and transparent experience is what makes us special. Our business materials provide a simple and transparent basis for decision-making, and we serve our end customers locally, worldwide. As a whole, any.cloud's partners through distribution experience a secure and close working partnership with the company based on an empathetic and personal relationship with our employees.

We are a strong international team with offices in a number of countries.

We are ISO 27001 certified, and we make continuous improvements to policies, procedures, practical operations, and physical and logical security.

Nature of the processing

any.cloud's processing of personal data on behalf of the data controller relates to data protection and storage, including backup and disaster recovery of the following platforms:

- any.cloud Backup for 365 & Arrow Cloud Backup for 365
- any.cloud Backup for Azure
- any.cloud BaaS for Veeam
- any.cloud Disaster Recovery for Veeam
- Arrow Cloud Object Storage for Backup

The purpose of processing personal data on the backup platforms mentioned above is to store data as a backup. All data is stored end-2-end encrypted with data encrypted "at-rest".

Information security strategy

any.cloud works on the basis of a standardised ISO 27001 IT security framework. This is used to avoid risks in IT security and threats to any.cloud services.

Retention of this, as well as ISAE 3000, is an important and necessary part of the delivery of all of any.cloud's services internationally.

All information is treated with the necessary confidentiality, solely from approved transactions in accordance with ISO 27001 and ISAE 3000.

All supporting systems and employees for any.cloud services are considered critical resources. Emphasis is therefore placed on the quality of the operation and its security. any.cloud's information security policy helps to create a secure safeguard against IT security threats, so that data security and credibility are maintained. In the information security strategy, emphasis is placed on natural, technical, and man-made threats.

The EU General Data Protection Regulation provides the framework for the legal processing of personal data in any.cloud. Data processing agreements are entered into between all partners and any.cloud.

We are responsible for taking the necessary technical and organisational measures to ensure that all personal data are processed in a correct and responsible manner.

In order to comply with the EU General Data Protection Regulation, we have chosen to standardise all deliveries via ISO 27001 and ISAE 3000.

The process for both is repeated annually and results in a assurance report and a renewed certificate. This declaration can also be used to contribute to any.cloud's partners' monitoring of whether any.cloud complies with the instructions that have been entered into in the data processing agreements.

any.cloud has chosen to use the following areas to support personal data and information security:

- Organisation and responsibilities
- Risk assessment and management
- Security policy
- Organisation of information security
- HR-related security
- Asset management
- Access management
- Cryptography
- Physical safety and environmental protection
- Operational security
- Communication security
- Acquisition, development, and maintenance of systems
- Management of information security breaches
- Compliance

The above areas are included in any.cloud's ISMS for ISO 27001.

Instructions from the data controller

any.cloud only processes personal data on written instructions from the data controller via the any.cloud ticket system. any.cloud will immediately notify the data controller if a ticketed instruction violates the General Data Protection Regulation.

Risk management in any.cloud

any.cloud has implemented risk management and a risk management policy, which monitors all activities and identifies whether there are risks that must be dealt with or limited to an extent that maintains normal operations.

any.cloud has incorporated processes and procedures for risk management throughout the business. These are performed periodically and when changes are made to the operating systems or the business. Each implementation also includes a risk analysis to ensure that new systems meet any.cloud's requirements.

Assets

All any.cloud's assets are managed on an ongoing basis and fixed processes for employment and resignation are prepared to ensure that assets remain in any.cloud's care. All assets are centrally managed via internal software to ensure security.

Information security policy

The management of any.cloud has the day-to-day responsibility for ensuring the IT security that has been chosen and the accompanying requirements. The information security policy is revised at least annually.

The information security policy is created based on the ISO 27001 framework and follows all the points in it. It is designed to apply to all employees involved in the operation and delivery of any.cloud, and an ISMS can be presented to support this.

All systems are documented in any.cloud. All changes are logged, and all configuration files are stored securely and are accessible.

Everyone at any.cloud therefore works on the basis of a common set of rules and procedures. This provides a stable operating environment and a high level of security. All procedures and processes are continuously revised and improved to ensure stable and secure delivery of all services and processing of personal data.

any.cloud's organisational structure

any.cloud A/S is owned by ANY A/S and has 40+ employees. any.cloud provides service to partners and their end customers in more than 30 countries.

ANY A/S owns 100% of any.cloud A/S.

any.cloud's organisational structure:

Management:
Responsible for the day-to-day operation of any.cloud.

Sales:
Responsible for all sales, product demonstrations, submission of offers and processing of orders.

Marketing:
Responsible for all social media, visual identity, co-marketing activities and external communication.

Service & Delivery:
Handles all partners and services, commercial operations and supports any.cloud's partners.

Operation:
Responsible for all technical operation of any.cloud's platforms and related services.

Development:
Responsible for the development of all of any.cloud's services.

Support:
Provides support for all any.cloud services to its partners.

HR security

any.cloud's employees are the most important resource and the key to a secure and stable delivery of all any.cloud services. any.cloud is subject to processes and internal requirements for its employees and their knowledge and know-how within information security.

There are therefore six-monthly in-house awareness training courses, as well as requirements for other staff training.

any.cloud's employees have signed non-disclosure agreements that also relate to the processing of data and its confidentiality.

Accessibility

Only authorised personnel have access to any.cloud's systems. Access is granted via any.cloud's COO and based on an approval process that ensures that access is only given to the correct personnel. Rights are managed based on the roles held by our employees.

Operational security

any.cloud has implemented an operating procedure for information and communication technology safeguarding standards within:

- Change management
- Backup
- Network security management
- Cloud services
- Disposal and destruction of equipment and media
- Transfer of information
- System monitoring
- Logging
- Patch management

Cryptography

Access to all services for all any.cloud employees is always encrypted, mostly via TLS.

Network security management

any.cloud's operations department is responsible for managing all operational networks to ensure the security of information in networks and to protect the services connected to the network from unauthorised access.

For any.cloud's operations department it is therefore necessary:

- To have operational responsibility for networks and responsibility for sensitive applications and other systems.
- To protect sensitive data passing over the public network by always using closed networks or encrypted lines.
- To protect sensitive data using wireless networks by using only networks to which only authorised personnel have access.
- To protect equipment connecting the network from remote locations by restricting access to them with personal access, which can only take place over approved networks via encrypted connections.
- To separate traffic from mobile devices, create unique firewall policies, static routes, virtual local networks, etc.
- To ensure availability of network services by always using redundant equipment.

Cloud services

any.cloud's COO, together with any.cloud's operations department, is responsible for managing and controlling the infrastructure, platforms and services, security levels and features driving any.cloud's operations/and cloud environment, whether these are operated internally or externally.

All cloud environments that are part of the delivery for any.cloud services are subject to any.cloud's security requirements for ISO 27001.

Disposal and destruction of equipment, media, and data

For logical deletions, any.cloud has implemented a procedure to ensure the secure deletion of data that supports EU data legislation.

System monitoring

Based on the result of the risk assessment, any.cloud's COO determines which log files are to be stored on which systems, for which systems and for how long they will be stored. Log files must be stored for all user and administrator log-ins.

any.cloud's operations department is responsible for monitoring the log files for automatically reported errors every day, as well as for detecting errors reported by users, analysing why errors occurred, and taking appropriate corrective action.

Logging

any.cloud ensures logging of all activities and proactively reacts if an abnormality is discovered. Based on the risk assessment, control is exercised over which activities on any.cloud's services are to be monitored. any.cloud has divided logs into two levels:

- System log: any.cloud's own internal system for monitoring logs
- User log: All any.cloud partners have access to their services and to these portals, which contain logs of user-specific activities.

Patch management

any.cloud has implemented a patch management system that ensures that patches are implemented on time while ensuring that critical security updates are implemented as quickly as possible to minimise risks.

Development environment

any.cloud has implemented testing and staging environments where all software is tested before being put into operation.

Security incident management

any.cloud has implemented procedures for incidents and deviations, including security breaches.

These ensure that work is carried out systematically and that necessary data collection and documentation is carried out, which are used both internally and externally, in the form of incident reports.

any.cloud's management is responsible for this process and its operating personnel for carrying out this work.

Incident management

any.cloud has incorporated a procedure in accordance with the ISO 27001 standard for incident management.

Ongoing checks

All any.cloud procedures, policies and risk assessment are checked on an ongoing basis, in accordance with an interval established based on the ISO 27001 standard.

Data Protection Officer (DPO)

any.cloud has currently chosen not to have a DPO in the light of the nature of the business and services, as well as the type of data that any.cloud processes.

Compliance with security policies and standards

Our employees read the IT security policy at least once a year in the event of changes. We have ongoing checks by our management to ensure that our employees comply with the security measures specified in our IT security policy, which applies to both the physical and logical conditions.

Compliance with the role of data processor

any.cloud's management is responsible for all relevant legal and contractual requirements that are identified and that these are complied with correctly. Examples of these include:

- The EU General Data Protection Regulation
- Local legislation on data protection
- Data processor agreements (DPAs)
- any.cloud's terms and conditions for its services
- any.cloud's EULA for its services

The EU General Data Protection Regulation (GDPR)

All of any.cloud's solutions support the GDPR. any.cloud does not own the data collected on behalf of its partner's customers, but only develops and operates services that the partners use to perform the necessary personal data processing. Any any.cloud customer with the contractual relationship is considered the data controller and any.cloud is considered as being the data processor.

Data processing agreement

As a data processor, any.cloud is subject to liability under the General Data Protection Regulation, which is why a data processing agreement is required. any.cloud must therefore, among other things:

- Describe the technical and organisational security measures that have been established to protect personal data on any.cloud's services.
- Contribute to fulfilling the customer's obligations regarding the rights of the data subject.
- Provide the customer with expertise to ensure compliance with:
    - Article 32 – Security of Processing
    - Article 33 – Reporting Personal Data Breaches
    - Article 34 – Notification of Personal Data Breaches for Data Subjects
- Inform the customer of the name and contact details of the supplier, which may be sub-processors.
- Ensure that any requirements from the customer are also reflected by the sub-processor.

As a data processor, any.cloud works with personal data on the basis of instructions from the customers, which describe the purpose for which the data may be used. any.cloud is responsible for ensuring that data is collected solely for this purpose.

Transfer of personal data

any.cloud will not transfer any data to third countries. However, the customer may choose to use any.cloud's administration portals to transfer data to a third country. This is done exclusively on the customer's own instructions and any.cloud will transfer data to a third country at its own behest.

Access to customer data

any.cloud services are SaaS solutions operated by any.cloud. any.cloud handles tests and releases itself. any.cloud therefore has full responsibility for processing customer data. In general, the employees in any.cloud do not have access to the customer's data, unless this concerns specific personnel where access is considered necessary to be able to operate the platform. Only Operations and any.cloud's management have access to customers' data, which is nevertheless encrypted.

Records

any.cloud has records of all its services, so that an overview is maintained of the type of personal data that is processed, and that this is done in accordance with any.cloud's information security policies.

Complementary controls carried out by data controllers

Data controllers have the following obligations:

- to ensure that personal data is up to date,
- to ensure that the instructions are legal in relation to the personal data legislation in force at any time,
- to ensure that the instructions are appropriate in terms of this data processing agreement and the main service,
- to ensure that the data controller's users are up to date,
- to ensure that the necessary legal basis for processing is in place,
- to comply with the duty to inform the data subjects about the exercise of their rights,
- to verify the identity of data subjects wishing to exercise their rights.

Section 4: Control objectives, controls, tests, and results hereof

We conducted our engagement in accordance with ISAE 3000, assurance engagements other than audits or review of historical financial information.

Our test of the functionality has included the control objectives and attached controls, selected by management and which are stated in the control objectives A-I below. Our test has included the controls, we find necessary to establish reasonable assurance for compliance with the articles stated throughout the period from 20 April 2023 to 19 April 2024.

Further, controls performed at the data controller are not included in this statement.

We performed our test of controls at any.cloud A/S by the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at any.cloud A/S. The interviews have included questions about, how controls are performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

List of control objectives compared to GDPR-articles, ISO 27701, and ISO 27001/2

Below, control objectives are mapped against the articles in GDPR, ISO 27701 and ISO 270001/2. Articles and points about main areas are written in bold.

Control activity	GDPR articles	ISO 27701	ISO 27001/2:2013
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*New scope compared to ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*New scope compared to ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*New scope compared to ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*New scope compared to ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*New scope compared to ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*New scope compared to ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Control objective A - Instructions regarding processing of personal data

Procedures and controls are complied with to ensure that instructions for the processing of personal data are complied with consistently with the data processing agreement entered into.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
A.1	Written procedures exist which include a requirement that personal data must only be processed when instructions to this effect are available. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only processed according to instructions. We have inspected that the procedures include a requirement to, at least once a year, assess the need for updates, including in case of changes in the data controller's instructions or changes in the data processing. We have inspected that procedures are up to date.	No deviations noted.
A.2	The data processor only processes personal data stated in the instructions from the data controller.	We have inspected that management ensures that personal data are only processed according to instructions. We have, by sample test, inspected personal data processing operations are conducted consistently with instructions.	No deviations noted.
A.3	The data processor immediately informs the data controller if an instruction, in the data processor's opinion, infringes the Regulation or other European Union or member state data protection provisions.	We have inspected that formalised procedures exist ensuring verification that personal data are not processed against the Regulation or other legislation. We have inspected that procedures are in place for informing the data controller of cases where the processing of personal data is evaluated to be against legislation. We have inquired whether the data processor has received instructions which, in the data processor's opinion, contravene the data protection regulation or data protection provisions in other EU law or their national law.	We have been informed that the data processor has not received instructions which, in the data processor's opinion, contravene the data protection regulation or data protection provisions in other EU law or the national law of the Member States, which is why we have not tested the effectiveness of relevant procedures. No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.1	Written procedures exist which include a requirement that safeguards agreed are established for the processing of personal data in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that there are formalised procedures that ensure that the agreed security measures are established. We have inspected that procedures are up to date.	No deviations noted.
B.2	The data processor has performed a risk assessment and based on this, implemented the technical measures considered relevant to achieve an appropriate level of security, including establishment of the safeguards agreed with the data controller.	We have inspected that formalised procedures are in place to ensure that the data processor performs a risk assessment to achieve an appropriate level of security. We have inspected that the risk assessment performed is up to date and includes the current processing of personal data. We have inspected that the data processor has implemented the technical measures ensuring an appropriate level of security consistent with the risk assessment. We have inspected that the data processor has implemented the safeguards agreed with the data controller.	No deviations noted.
B.3	For the systems and databases used in the processing of personal data, antivirus software has been installed that is updated on a regular basis.	We have inspected that, for the systems and databases used in the processing of personal data, antivirus software has been installed.	No deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.6	Access to personal data is isolated to users with a work-related need for such access.	We have inspected that formalised procedures are in place for restricting users' access to personal data. We have inspected that formalised procedures are in place for following up on users' access to personal data being consistent with their work-related need. We have inspected that an access policy is in place. We have inspected that access is restricted to the employees' work-related needs.	We have inspected that there is no formalised procedure for users' access to personal data. However, we have inspected that an access policy exists. No further deviations noted.
B.8	Effective encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that formalised procedures are in place to ensure that transmissions of sensitive and confidential data through the internet are protected by powerful encryption based on a recognised algorithm. We have inspected that technological encryption solutions have been available and active throughout the assurance period. We have inspected that encryption is applied when transmitting confidential and sensitive personal data through the internet or by email.	We have inspected that on a single domain, personal data are transmitted via the Internet with an insecure TLS protocol. We have been informed that the domain has been planned to be decommissioned. No further deviations noted.
B.9	Logging has been established in systems, databases, and networks. Log data are protected against manipulation, technical errors and are reviewed regularly.	We have inspected that formalised procedures exist for setting up logging of user activities in systems, databases or networks that are used to process and transmit personal data. We have inspected that logging of user activities in systems, databases or networks that are used to process or transmit personal data, has been configured and activated. We have inspected that user activity data collected in logs are protected against manipulation or deletion.	We have inspected that there is a single employee who has access to make changes to logs. No further deviations noted.

Control objective B - Technical measures

Procedures and controls are complied with to ensure that the data processor has implemented technical measures to safeguard relevant security of processing.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
B.10	Personal data used for development, testing or similar activity are always in pseudonymised or anonymised form.	We have inspected that formalised procedures exist for using personal data for development, testing or similar activity to ensure that such use only takes place in pseudonymised or anonymised form. We have, by sample test, inspected that personal data included in development or test databases are pseudonymised or anonymised.	No deviations noted.
B.11	The technical measures established are tested on a regular basis in vulnerability scans and penetration tests.	We have inspected that formalised procedures exist for regularly testing technical measures, including for performing vulnerability scans. We have inspected samples that documentation exists regarding regular testing of the established technical measures.	No deviations noted.
B.12	Changes to systems, databases or networks are made consistently with procedures established that ensure maintenance using relevant updates and patches, including security patches.	We have inspected that formalised procedures exist for handling changes to systems, databases, or networks, including handling of relevant updates, patches, and security patches. We have inspected extracts from technical security parameters and setups that systems, databases, or networks have been updated using agreed procedures.	No deviations noted.
B.13	A formalised procedure is in place for granting and removing users' access to personal data. Users' access is reconsidered on a regular basis, including the continued justification of rights by a work-related need.	We have inspected that formalised procedures exist for granting and removing users' access to systems and databases used to process personal data. We have inspected that documentation exists that user accesses granted are evaluated and authorised on a regular basis – and at least once a year.	No deviations noted.
B.14	Systems and databases processing personal data that involve a high risk for the data subjects are accessed as a minimum by using two-factor authentication.	We have inspected that users' access to processing personal data that involve a high risk for the data subjects can only take place by using two-factor authentication.	No deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.1	Management of the data processor has approved a written information security policy that has been communicated to all relevant stakeholders, including the data processor's employees. The IT security policy is based on the risk assessment performed. Assessments are made on a regular basis – and at least once a year – as to whether the IT security policy should be updated.	We have inspected that an information security policy exists that management has considered and approved within the past year. We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the data processor's employees.	No deviations noted.
C.2	Management of the data processor has checked that the information security policy does not conflict with data processing agreements entered into.	We have inspected documentation of management's assessment that the information security policy generally meets the requirements for safeguards and the security of processing in the signed data processing agreements. We have, by sample test, inspected that the requirements in data processing agreements are covered by the requirements of the information security policy for safeguards and security of processing.	No deviations noted.
C.3	The employees of the data processor are screened as part of the employment process.	We have inspected that formalised procedures are in place to ensure screening of the data processor's employees as part of the employment process. We have, by sample test, inspected whether the screening procedure has been followed for new employees.	We have inspected that there is no background check documentation available for 5 out of 5 recently hired employees. No further deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.4	Upon appointment, employees sign a confidentiality agreement. In addition, the employees are introduced to the information security policy and procedures for data processing as well as any other relevant information regarding the employees' processing of personal data.	We have, by sample test, inspected that employees appointed during the assurance period have signed a confidentiality agreement. We have inspected that there are formalised procedures which ensure that newly hired employees sign a confidentiality agreement. We have inquired if employees appointed during the assurance period have been introduced to the information security policy and procedures for processing data and other relevant information.	No deviations noted.
C.5	For resignations or dismissals, the data processor has implemented a process to ensure that users' rights are deactivated or terminated, including that assets are returned.	We have inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal and that assets such as access cards, computers, mobile phones, etcetera are returned. We have, by sample test, inspected that rights have been deactivated or terminated and that assets have been returned for terminated employees during the assurance period.	No deviations noted.
C.6	Upon resignation or dismissal, employees are informed that the confidentiality agreement signed remains valid and that they are subject to a general duty of confidentiality in relation to the processing of personal data performed by the data processor for the data controllers.	We have inspected that formalised procedures exist to ensure that resigned or dismissed employees are made aware of the continued validity of the confidentiality agreement and the general duty of confidentiality. We have inquired if documentation exists of the continued validity of the confidentiality agreement and the general duty of confidentiality for employees resigned or dismissed during the assurance period.	We have inspected that in 2 out of 2 samples, the employee has not been informed about continuous validity of the confidentiality. No further deviations noted.

Control objective C - Organisational measures

Procedures and controls are complied with to ensure that the data processor has implemented organisational measures to safeguard relevant security of processing.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
C.7	Awareness training is provided to the data processor's employees on a regular basis with respect to general IT security and security of processing related to personal data.	We have inspected that the data processor provides awareness training to the employees covering general IT security and security of processing related to personal data. We have inspected documentation that all employees who have either access to, or process personal data have completed the awareness training provided.	No deviations noted.

Control objective D - Return and deletion of personal data

Procedures and controls are complied with to ensure that personal data are deleted or returned if arrangements are made with the data controller to this effect.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
D.1	Written procedures exist which include a requirement that personal data must be stored and deleted in accordance with the agreement with the data controller. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for storing and deleting personal data in accordance with the agreement with the data controller. We have inspected that the procedures are up to date.	No deviations noted.
D.2	Specific requirements have been agreed with respect to the data processor's storage periods and deletion routines.	We have inspected that the existing procedures for storage and deletion include specific requirements for the data processor's storage periods and deletion routines. We have, by sample test, inspected that documentation exists of personal data are stored in accordance with the agreed storage periods in data processing agreements.	We have been informed that no data processing has been terminated during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.

Control objective D - Return and deletion of personal data

Procedures and controls are complied with to ensure that personal data are deleted or returned if arrangements are made with the data controller to this effect.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
D.3	Upon termination of the processing of personal data for the data controller, data have, in accordance with the agreement with the data controller, been: • Returned to the data controller; and/or • Deleted if this is not in conflict with other legislation.	We have inspected that formalised procedures are in place for processing the data controller's data upon termination of the processing of personal data. We have inquired about whether data processing has been terminated during the declaration period.	We have been informed that no data processing has been terminated during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
G.1	Written procedures exist which include a requirement that the data processor must only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures exist to ensure that personal data are only transferred to third countries or international organisations in accordance with the agreement with the data controller, by using a valid basis of transfer. We have inspected that procedures are up to date.	No deviations noted.
G.2	The data processor must only transfer personal data to third countries or international organisations according to instructions by the data controller.	We have inquired into whether the data processor has transferred personal data to third countries or international organisations.	We have been informed that personal data are not transferred to third countries or international organisations, hence, this control is not relevant. No deviations noted.

Control objective G – Transfer of personal data to third countries

Procedures and controls are complied with to ensure that the data processor will only transfer personal data to third countries or international organisations in accordance with the agreement with the data controller by using a valid basis of transfer.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
G.3	As part of the transfer of personal data to third countries or international organisations, the data processor assessed and documented the existence of a valid basis of transfer.	We have inspected that formalised procedures are in place for ensuring a valid basis of transfer. We have inspected that procedures are up to date. We have, by sample test, inspected that documentation exists of a valid basis of transfer in the data processing agreement with the data controller and that transfers have only taken place as far as this was arranged with the data controller.	We have been informed that personal data are not transferred to third countries or international organisations, hence, the control is not relevant. No deviations noted.

Control objective H – Rights of the data subjects

Procedures and controls are complied with to ensure that the data processor can assist the data controller in handing out, correcting, deleting, or restricting information on the processing of personal data to the data subject.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
H.1	Written procedures exist which include a requirement that the data processor must assist the data controller in relation to the rights of data subjects. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place for the data processor's assistance to the data controller in relation to the rights of data subjects. We have inspected that procedures are up to date.	No deviations noted.
H.2	The data processor has established procedures as far as this was agreed that enable timely assistance to the data controller in handing out, correcting, deleting, or restricting or providing information about the processing of personal data to data subjects.	We have inspected that the procedures in place for assisting the data controller include detailed procedures for: • Handing out data • Correcting data • Deleting data • Providing information about the processing of personal data to data subjects. We have inspected documentation that the systems and databases used support the performance of the relevant detailed procedures. We have inquired into whether the data processor has received requests from the data controller in relation to the rights of the data subjects.	We have been informed that the data processor has not received requests from the data controller in relation to the data subjects' rights, wherefore we have not been able to test the effectiveness of the control. No deviations noted.

Control objective I – Managing personal data breaches

Procedures and controls are complied with to ensure that any personal data breaches are responded to in accordance with the data processing agreement entered into.

No.	*any.cloud A/S' control activity*	*Test performed by Grant Thornton*	*Result of test*
I.1	Written procedures exist which include a requirement that the data processor must inform the data controllers in the event of any personal data breaches. Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.	We have inspected that formalised procedures are in place which include a requirement to inform the data controllers in the event of any personal data breaches. We have inspected that procedures are up to date.	No deviations noted.
I.2	The data processor has established controls for identification of possible personal data breaches.	We have inspected that the data processor provides awareness training to the employees in identifying any personal data breaches. We have inquired if logging of access to personal data, is followed up on, on a timely basis.	We have inspected that there is a single employee who has access to make changes to logs. No further deviations noted.
I.3	If any personal data breach occurred, the data processor informed the data controller without undue delay after having become aware of such personal data breach at the data processor or a sub-data processor.	We have inquired whether there has been a breach of personal data security during the period.	We have been informed that there have been no personal data security breaches during the declaration period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.
I.4	The data processor has established procedures for assisting the data controller in filing reports with the Danish Data Protection Agency: • Nature of the personal data breach • Probable consequences of the personal data breach • Measures taken or proposed to be taken to respond to the personal data breach.	We have inspected that the procedures in place for informing the data controllers in the event of any personal data breach, include detailed procedures for: • Describing the nature of the personal data breach • Describing the probable consequences of the personal data breach • Describing measures taken or proposed to be taken to respond to the personal data breach. We have inspected documentation that the procedures available support that measures are taken to respond to the personal data breach.	No deviations noted.